IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Martina Hanck et al.
Serial No.:	09/402,144
Date Filed:	September 29, 1999
Examiner:	Kim, Jung W
Group Art Unit:	2132
Confirmation No.:	5593
Title:	**METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS**

Mail Stop – Appeal Brief--Patents
Honorable Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

Dear Sir:

REPLY BRIEF

Appellants have appealed to this Board from the final rejection of Claims 1-3, 10-12, 22-33 and 37-48 dated June 27, 2007 and Notice of Panel Decision from Pre-Appeal Brief Review dated November 28, 2007. Appellants mailed a Notice of Appeal on September 27, 2007 and filed an Appeal Brief on January 28, 2008 (the *"Appeal Brief"*). The Examiner responded in an Examiner's Answer mailed May 29, 2008 (the *"Examiner's Answer"*). Appellants respectfully submit this Reply Brief.

In the *Examiner's Answer*, the Examiner sustained the final rejection.

I.   REAL PARTY IN INTEREST

This application is currently owned by Siemens Aktiengesellschaft, as indicated by an assignment recorded on February 3, 1998, in the Assignment Records of the United States Patent and Trademark Office at Reel 010411, Frame 0669.

II.   RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision regarding this appeal.

III.   STATUS OF CLAIMS

Claims 1-3, 10-12, 22-33 and 37-48 are pending in this application. Claims 4-9, 13-21 and 34-36 have been canceled. Claims 1-3, 10-12, 22-33 and 37-48 stand rejected under a Final Office Action mailed June 27, 2007. No claims have been allowed. Appellant's presents Claims 1-3, 10-12, 22-33 and 37-48 for appeal. Appendix A shows all pending claims.

IV.   STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

A summary of the invention by way of reference to the drawings and specification for each of the independent claims and each means plus function claim may be found in Appendix B to this Brief.

Although specification citations are given in accordance with C.F.R. 1. 192(c), these reference numerals and citations are merely examples of where support may be found in the specification for the terms used in this section of the Brief. There is no intention to suggest in any way that the terms of the claims are limited to the examples in the specification. As demonstrated by the references numerals and citations below, the claims are fully supported

by the specification as required by law. However, it is improper under the law to read limitations from the specification into the claims. Pointing out specification support for the claim terminology as is done here to comply with rule 1.192(c) does not in any way limit the scope of the claims to those examples from which they find support. Nor does this exercise provide a mechanism for circumventing the law precluding reading limitations into the claims from the specification. In short, the references numerals and specification citations are not to be construed as claim limitations or in any way used to limit the scope of the claims.

Claim 1

With reference to the figure, claim 1 recites a method for securely controlling transmission of digital data (pg. 9, lines 7-12). The method includes the steps of receiving said digital data (pg. 7, lines 4-9), grouping said digital data into a number of data segments by a computer (pg. 7, lines 14-16), forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), forming a first commutative checksum by a commutative operation on said first segment checksums (pg, 7, lines 20-25), wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and cryptographically protecting said first commutative checksum by using a cryptographic operation (pg. 7, lines 24-30).

Claim 2

With reference to the figure, claim 2 recites a method for securely controlling transmission of digital data (pg. 9, lines 7-12). The method includes the steps of receiving said digital data (pg. 7, lines 4-9), grouping the digital data into a number of data segments by a computer (pg. 7, lines 14-16), allocating a predetermined cryptographic commutative checksum to said digital data (pg 7, lines, 16-20), subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum (pg. 7, lines 24-30 and pg 8, lines 13-18), forming a second segment checksum

for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 8, lines 7-12 and pg 10, lines 1-8), forming a second commutative checksum by a commutative operation on said second segment checksums (pg 9, lines 1-3), wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and checking said second commutative checksum for a match with said first commutative checksum. (pg. 9, lines 4-6).

Claim 3

With reference to the figure, claim 3 recites a method for forming and checking a first commutative checksum for digital data (pg. 9, lines 4-6). The method includes the steps of grouping said digital data into a number of data segments by a computer (pg. 7, lines 14-16), forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), forming said first commutative checksum by a commutative operation on said first segment checksums (pg, 7, lines 20-25), wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), cryptographically protecting said first commutative checksum by using at least one cryptographic operation, which forms a cryptographic commutative checksum (pg. 7, lines 24-30), subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum (pg 8, lines 13-18), forming a second segment checksum for each said data segment of said digital data to which said first commutative checksum is allocated (pg 8, lines 7-12 and pg 10, lines 1-8), forming a second commutative checksum by a commutative operation on said second segment checksums (pg. 9, lines 1-3), wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and checking said second commutative checksum for a match with said reconstructed first commutative checksum (pg. 9, lines 4-6).

Claim 10

With reference to the figure, claim 10 recites an arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments (pg 7, lines 16-25). The arrangement includes an arithmetic and logic unit (R; pg 7, lines 10-15), a first segment checksum (PS1-PSn; pg. 7, lines 16-20), which is formed for each said data segment in accordance with a type selected :from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), a commutative operation which forms said first commutative checksum by operating on said segment checksums (101; pg 7, lines 3135) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and a cryptographic operation which cryptographically protects said first commutative checksum (pg. 7, lines 24-30).

Claim 11

With reference to the figure, claim 11 recites an arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments (pg 9, lines 4-6). The arrangement includes an arithmetic and logic unit (R; pg 7, lines 10-15), a first segment checksum (PS1-PSn; pg. 7, lines 16-20), formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), an inverse cryptographic operation to form a first cryptographic checksum :from a cryptographic commutative checksum formed by a cryptographic operation (pg. 7, lines 24-30) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), a second segment checksum which is formed for each said data segment wherein said second segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (PSa-Psz; pg

8, lines 7-12 and pg 10, lines 1-8), a commutative operation which operates on said second segment checksums which forms a second commutative checksum (pg 9, lines 1-3) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and a comparator which checks for a match between said second commutative checksum and said first commutative checksum (pg 9, lines 4-6).

Claim 12.

With reference to the figure, claim 12 recites an arrangement for forming and checking a first commutative checksum for digital data which is grouped into a number of data segments (pg. 9, lines 4-6). The arrangement includes an arithmetic and logic unit (R; pg 7, lines 10-15), a first segment checksum (PS1-PSn; pg. 7, lines *16-20),* which is formed for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, *16-20* and pg 10, lines 1-7), a commutative operation which forms said first commutative checksum by operating on said first segment checksums(101; pg 7, lines 31-35) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), a cryptographic operation which cryptographically protects said first commutative checksum (pg. 7, lines *24-30),* a cryptographic commutative checksum formed by said cryptographic operation (KP; pg 7, lines *26-30);* an inverse cryptographic operation to form a first commutative checksum from said cryptographic commutative checksum (pg. 7, lines *24-30),* a second segment checksum which is formed for each said data segment of said digital data to which said first commutative checksum is allocated (pg 8, lines 7-12 and pg. 10, lines 1-8), a commutative operation which operates on said second segment checksums which forms a second commutative checksum (pg. 9, lines 1-3) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and a comparator which checks for a match between said second commutative checksum and a reconstructed first commutative checksum (pg 9, lines 4-6), wherein said first and second segment checksum

are formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg. 10, lines 1-8).

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-3, 10-12, 22-33 and 37-48 stand rejected under 35 USC §103(a) as being unpatentable over USPN 5,649,089 to Kilner in view of USPN 4,982,430 to Frezza; the subject matter of USPN to McNamara et al. is relied upon since McNamara is incorporated by reference in Frezza.

VII.   ARGUMENT

In addition to the argument presented in the Appeal Brief which are hereby incorporated by reference, Appellants reply to the Examiner's Answer as follows: The Examiner maintains his position that *Kilner* in view of *Frezza* renders the present claims obvious. Applicant respectfully disagrees.

The Examiner stated that *Kilner* does not disclose a cryptographic operation to protect the first commutative checksum. However, the Examiner further stated that *Frezza* teaches encrypting integrity values prior to submitting the integrity value over a network link to prevent unauthorized alteration of a message. The Examiner then concluded that it would be obvious to one of ordinary skill in the art to modify the invention of *Kilner* by including a cryptographic operation to secure the first commutative checksum. Applicant respectfully disagrees.

To enhance security, *Frezza* teaches to apply a cryptographic method on data which is transmitted via a network between a network and a subscriber. *Frezza, 2:45-51. Frezza,* thus, specifically teaches to send the terminal software encrypted from the service provider to the subscriber terminal. *Id. Frezza* further states that a checksum can be sent back to the service provider to verify a correct transmission and if encryption is used that this checksum can also be encrypted. *Frezza, 2:52-57.* However, *Frezza* merely proposes this because this confirmation using the checksum is the only communication back to the service provider and no other protection means would exist. However, in a scenario as taught by *Kliner,* the primarily transferred information are the data records. Hence, a person skilled in the art, in order to improve security of the system disclosed in *Kilner,* would apply such a cryptographic method to each data segment to prevent decoding of the respective data. Once such an encryption has been established, a person skilled in the art would have no reason to also apply this encryption to a checksum. Rather, a person skilled in the art would follow the teaching of *Kilner* and form a cumulative checksum on the checksums of the encrypted data. Because encrypted data segments cannot be decoded without knowing the encryption key, the security would be enhanced and no further encryption of the cumulative checksum would be necessary. Thus, it is not obvious from *Kilner* in view of *Frezza* to only apply the encryption

to the cumulative checksum. This is in particular true because *Frezza* neither discloses segmented checksums let alone a cumulative checksum.

Contrary to this the present independent claims include features that allow for an easier way to enhance the security which requires less data processing. Only the commutative checksum will be cryptographically encoded. Thus, for a plurality of data segments for which a commutative checksum is formed, a significant processing time can be saved.

Therefore, Appellants respectfully request allowance of all independent claims. Appellants respectfully submit that the dependent Claims are allowable at least to the extent of the independent Claim to which they refer, respectively. Thus, Appellants respectfully request reconsideration and allowance of the dependent Claims.

SUMMARY

Appellants have demonstrated that the present invention, as claimed, is patentable over the prior art cited by the Examiner. Therefore, Appellants respectfully request the Board to reverse the final rejections and instruct the Examiner to issue a Notice of Allowance with respect to all pending claims.
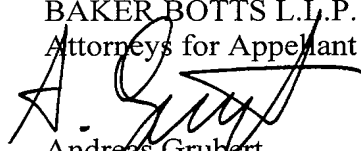
Appellants authorize The Commissioner to charge the fee of $510.00 for the filing of the Reply Brief to Deposit Account 50-2148 in order to effectuate this filing.

Although Appellants believe no additional fees are due, the Commissioner is hereby authorized to charge any additional fees and credit any overpayments to Deposit Account No. 50-2148 of Baker Botts L.L.P.

If there are any matters concerning this Application that may be cleared up in a telephone conversation, please contact Applicant's attorney, Andreas Grubert, at 512.322.2545.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Appellant

Andreas Grubert
Reg. No. 59,143

Date: July 8, 2008

CORRESPONDENCE ADDRESS:
CUSTOMER NO. **31625**
(512)322-2545
(512)322-8383 (fax)

APPENDIX A - CLAIMS INVOLVED IN APPEAL

Claim 1. A method for securely controlling transmission of digital data comprising the steps of:

receiving said digital data;

grouping said digital data into a number of data segments by a

computer;

forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

forming a first commutative checksum by a commutative operation on said first segment checksums, wherein flow control for the data segments is negated by the commutative operation; and

cryptographically protecting said first commutative checksum by using a cryptographic operation.

Claim 2. A method for securely controlling transmission of digital data comprising the steps of:

receiving said digital data;

grouping the digital data into a number of data segments by a computer;

allocating a predetermined cryptographic commutative checksum to said digital data;

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum;

forming a second segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

forming a second commutative checksum by a commutative operation on said second segment checksums wherein flow control for the data segments is negated by the commutative operation; and

checking said second commutative checksum for a match with said first

commutative checksum.

Claim 3. A method for forming and checking a first commutative checksum for digital data comprising the steps of:

grouping said digital data into a number of data segments by a computer;

forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

forming said first commutative checksum by a commutative operation on said first segment checksums, wherein flow control for the data segments is negated by the commutative operation;

cryptographically protecting said first commutative checksum by using at least one cryptographic operation, which forms a cryptographic commutative checksum;

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum;

forming a second segment checksum for each said data segment of said digital data to which said first commutative checksum is allocated;

forming a second commutative checksum by a commutative operation on said second segment checksums wherein flow control for the data segments is negated by the commutative operation; and

checking said second commutative checksum for a match with said reconstructed first commutative checksum.

Claims 4-9 (canceled).

Claim 10. An arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit,

a first segment checksum, which is formed for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function,

a commutative operation which forms said first commutative checksum by

operating on said segment checksums wherein flow control for the data segments is negated by the commutative operation, and

a cryptographic operation which cryptographically protects said first commutative checksum.

Claim 11. An arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit;

a first segment checksum, formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation wherein flow control for the data segments is negated by the commutative operation;

a second segment checksum which is formed for each said data segment, wherein said second segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

a commutative operation which operates on said second segment checksums which

forms a second commutative checksum wherein flow control for the data segments

is negated by the commutative operation; and
a comparator which checks for a match between said second commutative checksum and said first commutative checksum.

Claim 12. An arrangement for forming and checking a first commutative checksum for digital data which is grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit,

a first segment checksum, which is formed for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function,

a commutative operation which forms said first commutative checksum by operating on said first segment checksums wherein flow control for the data segments is negated by the

commutative operation,

a cryptographic operation which cryptographically protects said first commutative checksum,

a cryptographic commutative checksum formed by said cryptographic operation,

an inverse cryptographic operation to *form* a first commutative checksum. :from said cryptographic commutative checksum.,

a second segment checksum. which is formed for each said data segment of said digital data to which said first commutative checksum. is allocated,

a commutative operation which operates on said second segment checksums which forms a second commutative checksum. wherein flow control for the data segments is negated by the commutative operation, and

a comparator which checks for a match between said second commutative checksum. and a reconstructed first commutative checksum., wherein said first and second segment checksum are formed in accordance with a type selected : from the group consisting of a hashing value and a cryptographic one-way function.

Claims 13- 21. (canceled).

Claim 22. A method according to claim 1, wherein:
said cryptographic operation is an operation selected :from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 23. A method according to claim 2, wherein:
said cryptographic operation is an operation selected : from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 24. A method according to claim 3, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an symmetric cryptographic method.

Claim 25. A method according to claim 1, wherein:

said commutative operation exhibits the property of associativity.

Claim 26. A method according to claim 2, wherein:

said commutative operation exhibits the property of associativity.

Claim 27. A method according to claim 3, wherein:

said commutative operation exhibits the property of associativity.

Claim 28. A method according to claim 1, wherein said digital data and the first cryptographic, commutative checksum are archived.

Claim 29. A method according to claim 2, wherein said digital data and the prescribed cryptographic commutative checksum have been
archived.

Claim 30. A method according to claim 3, wherein said digital data are secured which are processed corresponding to a network management protocol.

Claim 31. A method according to claim 1, further comprising the steps of:

protecting said digital data; and

processing said digital data in accordance with a network management protocol.

Claim 32. A method according to claim 2, further comprising the steps of:

protecting said digital data; and

processing said digital data in accordance with a network management protocol.

Claim 33. A method according to claim 3, further comprising the steps of:

protecting said digital data; and

processing said digital data in accordance with a network management protocol.

Claims 34-36. (canceled).

Claim 37. An arrangement according to claim 10, wherein: said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 38. An arrangement according to claim 11, wherein: said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 39. An arrangement according to claim 12, wherein: said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 40. An arrangement according to claim 10 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 41. An arrangement according to claim 11 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 42. An arrangement according to claim 12, wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 43. An arrangement according to claim 10, wherein: said digital data and the first cryptographic, commutative checksum are archived.

Claim 44. An arrangement according to claim 11, wherein: said digital data and the prescribed cryptographic commutative checksum have been archived.

Claim 45. An arrangement according to claim 12, wherein:

said digital data and the first cryptographic, commutative checksum are archived.

Claim 46. An arrangement according to claim 10, wherein:

said digital data are protected via an arrangement of said arithmetic and logic unit; and

said digital data are processed in accordance with a network management protocol.

Claim 47. An arrangement according to claim 11, wherein:

said digital data are protected via an arrangement of said arithmetic and logic unit; and

said digital data are processed in accordance with a network management protocol.

Claim 48. An arrangement according to claim 12, wherein:

said digital data are protected via an arrangement of said arithmetic and logic unit; and

said digital data are processed in accordance with a network management protocol.

APPENDIX B - EVIDENCE

.

NONE

APPENDIX C: RELATED PROCEEDINGS

NONE